

POMERANTZ LLP

Jennifer Pafiti (SBN 282790)

468 North Camden Drive

Beverly Hills, CA 90210

Telephone: (818) 532-6499

E-mail: jpafiti@pomlaw.com

- additional counsel on signature page -

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

NAFIZ TALUKDER, Individually and on
Behalf of All Others Similarly Situated,

Plaintiff,

vs.

YAHOO! INC., MARISSA A. MAYER, and
KENNETH A. GOLDMAN,

Defendants

Case No.

**CLASS ACTION COMPLAINT FOR
VIOLATION OF THE FEDERAL
SECURITIES LAWS**

JURY TRIAL DEMANDED

Plaintiff Nafiz Talukder (“Plaintiff”), individually and on behalf of all other persons similarly situated, by Plaintiff’s undersigned attorneys, for Plaintiff’s complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff’s own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff’s attorneys, which included, among other things, a review of the Defendants’ public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission (“SEC”) filings, wire and press releases published by and regarding Yahoo! Inc. (“Yahoo” or the “Company”), analysts’ reports and advisories about the Company, and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1
2 1. This is a federal securities class action on behalf of a class consisting of all persons other
3 than Defendants who purchased or otherwise acquired common shares of Yahoo between November
4 12, 2013 and December 14, 2016, both dates inclusive (the “Class Period”). Plaintiff seeks to recover
5 compensable damages caused by Defendants’ violations of the federal securities laws and to pursue
6 remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the “Exchange Act”)
7 and Rule 10b-5 promulgated thereunder.
8

9 2. Yahoo, together with its subsidiaries, is a multinational technology company that
10 provides a variety of internet services, including, *inter alia*, a web portal, search engine, Yahoo! Mail,
11 Yahoo! News, Yahoo! Finance, advertising, and fantasy sports. As of February 2016, Yahoo had an
12 estimated 1 billion monthly active users, roughly 280 million Yahoo! Mail users, and 205 million
13 monthly unique visitors to its sites and services.
14

15 3. Founded in January 1994, the Company was formerly known as “Jerry and David’s
16 Guide to the World Wide Web” and changed its name to Yahoo! Inc. in March 1994. Yahoo is
17 headquartered in Sunnyvale, California. The Company’s common stock trades on the Nasdaq Capital
18 Market (“NASDAQ”) under the ticker symbol “YHOO.”
19

20 4. On July 25, 2016, Verizon Communications, Inc. (“Verizon”) formally announced its
21 intent to acquire Yahoo’s internet business for \$4.8 billion.

22 5. Throughout the Class Period, Defendants made materially false and misleading
23 statements regarding the Company’s business, operational and compliance policies. Specifically,
24 Defendants made false and/or misleading statements and/or failed to disclose that: (i) Yahoo’s
25 information security protocols were inadequate; (ii) Yahoo failed to encrypt its users’ personal
26 information and/or failed to encrypt its users’ personal data with an up-to-date and secure encryption
27 scheme; (iii) consequently, sensitive personal account information from more than 1 billion users was
28

1 vulnerable to theft; (iv) a data breach resulting in the theft of personal user data would foreseeably
2 cause a significant drop in user engagement with Yahoo's websites and services; and (v) as a result,
3 Yahoo's public statements were materially false and misleading at all relevant times.

4 6. On July 28, 2015, Ramses Martinez, Yahoo's interim Chief Information Security Officer
5 ("CISO"), posted a report on Yahoo's Tumblr blogging platform, entitled "Yahoo's Pays \$1M to
6 Network Vulnerability Reporters," describing the volume of security vulnerability reports that Yahoo
7 had received since initiating its Bug Bounty program, which Martinez described as "a feedback loop to
8 determine the effectiveness of our application security controls." Martinez's report stated, *inter alia*,
9 that Yahoo had received more than 10,000 submissions since the program's inception and had paid out
10 more than \$1 million to security vulnerability reporters.
11

12 7. Following Martinez's posting, Yahoo's share price fell \$0.17, or 0.45% over the
13 following two trading days, to close at \$36.67 on July 29, 2015.
14

15 8. Shortly thereafter, on August 4, 2015, Yahoo confirmed that a large-scale attack had
16 started on July 28, exploiting vulnerabilities in Yahoo's advertisements to spread malware to site
17 visitors.
18

19 9. On September 11, 2015, the online publication *TechCrunch* reported that Martinez had
20 "quietly left [Yahoo] in August for a security role at Apple."

21 10. On this news, Yahoo's share price fell \$1.11, or 3.53%, to close at \$30.32 on September
22 14, 2015, the following trading day.

23 11. On September 22, 2016, Yahoo disclosed that hackers had stolen information in late
24 2014 on more than 500 million accounts. Following the breach, Yahoo executives advised investors
25 that the breach was not material, in part because the Company had not required to reset their passwords.
26

27 12. On this news, Yahoo's share price fell \$1.35, or 3.06%, to close at \$42.80 on September
28 23, 2016.

13. On December 14, 2016, post-market, Yahoo announced that it had uncovered a data breach, stating that data from more than 1 billion user accounts was compromised in August 2013. In a press release and Current Report filed with the SEC on Form 8-K, Yahoo stated, in part:

SUNNYVALE, Calif., December 14, 2016— Yahoo! Inc. (NASDAQ:YHOO) has identified data security issues concerning certain Yahoo user accounts. Yahoo has taken steps to secure user accounts and is working closely with law enforcement.

As Yahoo previously disclosed in November, law enforcement provided the company with data files that a third party claimed was Yahoo user data. The company analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, ***Yahoo believes an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts.*** The company has not been able to identify the intrusion associated with this theft. Yahoo believes this incident is likely distinct from the incident the company disclosed on September 22, 2016.

For potentially affected accounts, the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system the company believes was affected.

Yahoo is notifying potentially affected users and has taken steps to secure their accounts, including requiring users to change their passwords. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.

Separately, Yahoo previously disclosed that its outside forensic experts were investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, the company believes an unauthorized third party accessed the company's proprietary code to learn how to forge cookies. The outside forensic experts have identified user accounts for which they believe forged cookies were taken or used. Yahoo is notifying the affected account holders, and has invalidated the forged cookies. The company has connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016.

(Emphases added.)

1 14. Following Yahoo's announcement, several news sources reported that Verizon was
2 considering ways to amend the terms of its deal with Yahoo to reflect the impact of the data breach and
3 would likely seek "major concessions" from Yahoo.

4 15. On this news, Yahoo's share price fell \$2.50, or 6.11%, to close at \$38.41 on December
5 15, 2016.

6 16. On December 15, 2016, after the market closed, the *Wall Street Journal* published an
7 article entitled "Yahoo's Password Move May Put Verizon Deal at Risk." The article stated, in part:

8 Yahoo Inc.'s move to force some users to reset their passwords following a newly
9 disclosed security breach could disrupt the planned sale of its core assets to Verizon
10 Communications Inc., security experts say.

11 Yahoo didn't force users to reset their passwords after its September disclosure of
12 another breach. *Experts say forcing users to reset their passwords typically causes some
13 to drop a service.*

14 That is one reason why the newly disclosed hack—which Yahoo says occurred in 2013
15 and affected more than one billion accounts—could prove more disruptive to Verizon's
16 pending \$4.83 billion acquisition of Yahoo's core assets.

17 ...

18 *Yahoo is forcing users to reset their passwords now because some of the material taken
19 in the 2013 breach wasn't encrypted, and other parts were protected by what is now
20 considered an outdated encryption scheme,* according to a person familiar with that
21 matter.

22 (Emphases added.)

23 17. On January 23, 2017, the *Wall Street Journal* reported that the SEC had opened an
24 investigation into the timing of Yahoo's disclosures regarding the data breaches. The article reported,
25 in part:

26 The Securities and Exchange Commission has opened an investigation, and in December
27 issued requests for documents, as it looks into whether the tech company's disclosures
28 about the cyberattacks complied with civil securities laws, the people said. The SEC
requires companies to disclose cybersecurity risks as soon as they are determined to have
an effect on investors.

1 The investigation is likely to center on a 2014 data breach at Yahoo that compromised the
2 data of at least 500 million users, according to the people familiar with the matter. Yahoo
3 disclosed that breach in September 2016, despite having linked the incident to state-
4 sponsored hackers two years earlier.

5 To date, Yahoo hasn't explained why the company took two years to disclose the 2014
6 incident publicly or who made the decision not to go public sooner with this information.
7 In mid-December Yahoo also said it had recently discovered an August 2013 data breach
8 that had exposed the private information of more than 1 billion Yahoo users.

9 18. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in
10 the market value of the Company's common shares, Plaintiff and other Class members have suffered
11 significant losses and damages.

12 JURISDICTION AND VENUE

13 19. The claims asserted herein arise under and pursuant to §§10(b) and 20(a) of the
14 Exchange Act (15 U.S.C. §§78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17
15 C.F.R. §240.10b-5).

16 20. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §1331
17 and §27 of the Exchange Act.

18 21. Venue is proper in this Judicial District pursuant to §27 of the Exchange Act (15 U.S.C.
19 §78aa) and 28 U.S.C. §1391(b). Yahoo's principal executive offices are located within this Judicial
20 District.

21 22. In connection with the acts, conduct and other wrongs alleged in this Complaint,
22 Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce,
23 including but not limited to, the United States mail, interstate telephone communications and the
24 facilities of the national securities exchange.

PARTIES

23. Plaintiff, as set forth in the accompanying Certification, purchased common shares of Yahoo at artificially inflated prices during the Class Period and was damaged upon the revelation of the alleged corrective disclosure.

24. Defendant Yahoo! Inc. is incorporated in Delaware, and the Company's principal executive offices are located at 701 First Avenue, Sunnyvale, California, 94089. Yahoo's common stock trades on the NASDAQ under the ticker symbol "YHOO."

25. Defendant Marissa A. Mayer ("Mayer") has served at all relevant times as the Company's Chief Executive Officer ("CEO") and Director.

26. Defendant Kenneth A. Goldman ("Goldman") has served at all relevant times as the Company's Chief Financial Officer ("CFO").

27. The Defendants referenced above in ¶¶ 25-26 are sometimes referred to herein as the "Individual Defendants."

SUBSTANTIVE ALLEGATIONS

Background

28. Yahoo, together with its subsidiaries, is a multinational technology company that provides a variety of internet services, including, *inter alia*, a web portal, search engine, Yahoo! Mail, Yahoo! News, Yahoo! Finance, advertising, and fantasy sports. As of February 2016, Yahoo had an estimated 1 billion monthly active users, roughly 280 million Yahoo! Mail users, and 205 million monthly unique visitors to its sites and services.

Materially False and Misleading Statements Issued During the Class Period

29. The Class Period begins on November 12, 2013, when Yahoo filed a Quarterly Report on Form 10-Q with the SEC, announcing the Company's financial and operating results for the quarter ended September 30, 2013 (the "Q3 2013 10-Q"). For the quarter, Yahoo announced net income of

1 \$296.66 million, or \$0.28 per diluted share, on revenue of \$1.14 billion, compared to net income of
2 \$3.12 billion, or \$2.64 per diluted share, on revenue of \$1.2 billion for the same period in the prior year.

3 30. In the Q3 2013 10-Q, with respect to the efficacy of the Company's encryption of user
4 data, Yahoo simply stated, in part:

5 *If our security measures are breached, our products and services may be perceived as*
6 *not being secure, users and customers may curtail or stop using our products and*
7 *services, and we may incur significant legal and financial exposure.*

8 Our products and services involve the storage and transmission of Yahoo's users' and
9 customers' personal and proprietary information in our facilities and on our equipment,
10 networks and corporate systems. Security breaches expose us to a risk of loss of this
11 information, litigation, remediation costs, increased costs for security measures, loss of
12 revenue, damage to our reputation, and potential liability. Our user data and corporate
13 systems and security measures have been and may in the future be breached due to the
14 actions of outside parties (including cyber attacks), employee error, malfeasance, a
combination of these, or otherwise, allowing an unauthorized party to obtain access to
our data or our users' or customers' data. Additionally, outside parties may attempt to
fraudulently induce employees, users, or customers to disclose sensitive information in
order to gain access to our data or our users' or customers' data.

15 Any breach or unauthorized access could result in significant legal and financial
16 exposure, increased remediation and other costs, damage to our reputation and a loss of
17 confidence in the security of our products, services and networks that could potentially
18 have an adverse effect on our business. Because the techniques used to obtain
19 unauthorized access, disable or degrade service, or sabotage systems change frequently or
20 may be designed to remain dormant until a predetermined event and often are not
21 recognized until launched against a target, we may be unable to anticipate these
22 techniques or implement adequate preventative measures. If an actual or perceived breach
23 of our security occurs, the market perception of the effectiveness of our security measures
24 could be harmed and we could lose users and customers.

25 31. The Q3 2013 10-Q contained signed certifications pursuant to the Sarbanes-Oxley Act of
26 2002 ("SOX") by the Individual Defendants, stating that the financial information contained in the Q3
27 2013 10-Q was accurate and disclosed any material changes to the Company's internal control over
28 financial reporting.

32. On February 28, 2014, Yahoo filed an Annual Report on Form 10-K with the SEC,
announcing the Company's financial and operating results for the quarter and year ended December 31,

1 2013 (the “2013 10-K”). For the quarter, Yahoo announced net income of \$348.19 million, or \$0.33
2 per diluted share, on revenue of \$1.27 billion, compared to net income of \$272.27 million, or \$0.23 per
3 diluted share, on revenue of \$1.35 billion for the same period in the prior year. For 2013, Yahoo
4 announced net income of \$1.37 billion, or \$1.26 per diluted share, on revenue of \$4.68 billion,
5 compared to net income of \$3.95 billion, or \$3.28 per diluted share, on revenue of \$4.99 billion for
6 2012.

7
8 33. In the 2013 10-K, with respect to the efficacy of the Company’s encryption of user data,
9 Yahoo simply stated, in part:

10 *If our security measures are breached, our products and services may be perceived as*
11 *not being secure, users and customers may curtail or stop using our products and*
12 *services, and we may incur significant legal and financial exposure.*

13 Our products and services involve the storage and transmission of Yahoo’s users’ and
14 customers’ personal and proprietary information in our facilities and on our equipment,
15 networks and corporate systems. Security breaches expose us to a risk of loss of this
16 information, litigation, remediation costs, increased costs for security measures, loss of
17 revenue, damage to our reputation, and potential liability. Security breaches or
18 unauthorized access have resulted in and may in the future result in a combination of
19 significant legal and financial exposure, increased remediation and other costs, damage to
20 our reputation and a loss of confidence in the security of our products, services and
21 networks that could have an adverse effect on our business. We take steps to prevent
22 unauthorized access to our corporate systems, however, because the techniques used to
23 obtain unauthorized access, disable or degrade service, or sabotage systems change
24 frequently or may be designed to remain dormant until a triggering event, we may be
25 unable to anticipate these techniques or implement adequate preventative measures. If an
26 actual or perceived breach of our security occurs, the market perception of the
27 effectiveness of our security measures could be harmed and we could lose users and
28 customers.

34. The 2013 10-K contained signed certifications pursuant to SOX by the Individual
Defendants, stating that the financial information contained in the 2013 10-K was accurate and
disclosed any material changes to the Company’s internal control over financial reporting.

35. On May 8, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
announcing the Company’s financial and operating results for the quarter ended March 31, 2014 (the

1 “Q1 2014 10-Q”). For the quarter, Yahoo announced net income of \$311.58 million, or \$0.29 per
2 diluted share, on revenue of \$1.13 billion, compared to net income of \$390.29 million, or \$0.35 per
3 diluted share, on revenue of \$1.14 billion for the same period in the prior year.

4 36. In the Q1 2014 10-Q, with respect to the efficacy of the Company’s encryption of user
5 data, Yahoo simply stated, in part:

6 *If our security measures are breached, our products and services may be perceived as*
7 *not being secure, users and customers may curtail or stop using our products and*
8 *services, and we may incur significant legal and financial exposure.*

9 Our products and services involve the storage and transmission of Yahoo’s users’ and
10 customers’ personal and proprietary information in our facilities and on our equipment,
11 networks and corporate systems. Security breaches expose us to a risk of loss of this
12 information, litigation, remediation costs, increased costs for security measures, loss of
13 revenue, damage to our reputation, and potential liability. Security breaches or
14 unauthorized access have resulted in and may in the future result in a combination of
15 significant legal and financial exposure, increased remediation and other costs, damage to
16 our reputation and a loss of confidence in the security of our products, services and
17 networks that could have an adverse effect on our business. We take steps to prevent
18 unauthorized access to our corporate systems, however, because the techniques used to
19 obtain unauthorized access, disable or degrade service, or sabotage systems change
20 frequently or may be designed to remain dormant until a triggering event, we may be
21 unable to anticipate these techniques or implement adequate preventative measures. If an
22 actual or perceived breach of our security occurs, the market perception of the
23 effectiveness of our security measures could be harmed and we could lose users and
24 customers.

25 37. The Q1 2014 10-Q contained signed certifications pursuant to SOX by the Individual
26 Defendants, stating that the financial information contained in the Q1 2014 10-Q was accurate and
27 disclosed any material changes to the Company’s internal control over financial reporting.

28 38. On August 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
announcing the Company’s financial and operating results for the quarter ended June 30, 2014 (the “Q2
2014 10-Q”). For the quarter, Yahoo announced net income of \$269.71 million, or \$0.26 per diluted
share, on revenue of \$1.08 billion, compared to net income of \$331.15 million, or \$0.30 per diluted
share, on revenue of \$1.14 billion for the same period in the prior year.

39. In the Q2 2014 10-Q, with respect to the efficacy of the Company's encryption of user data, Yahoo simply stated, in part:

If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.

Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.

40. The Q2 2014 10-Q contained signed certifications pursuant to SOX by the Individual Defendants, stating that the financial information contained in the Q2 2014 10-Q was accurate and disclosed any material changes to the Company's internal control over financial reporting.

41. On November 7, 2014, Yahoo filed a Quarterly Report on Form 10-Q with the SEC, announcing the Company's financial and operating results for the quarter ended September 30, 2014 (the "Q3 2014 10-Q"). For the quarter, Yahoo announced net income of \$6.77 billion, or \$6.70 per diluted share, on revenue of \$1.15 billion, compared to net income of \$296.66 million, or \$0.28 per diluted share, on revenue of \$1.14 billion for the same period in the prior year.

42. In the Q3 2014 10-Q, with respect to the efficacy of the Company's encryption of user data, Yahoo simply stated, in part:

If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.

Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.

43. The Q3 2014 10-Q contained signed certifications pursuant to SOX by the Individual Defendants, stating that the financial information contained in the Q3 2014 10-Q was accurate and disclosed any material changes to the Company's internal control over financial reporting.

44. On February 27, 2015, Yahoo filed an Annual Report on Form 10-K with the SEC, announcing the Company's financial and operating results for the quarter and year ended December 31, 2014 (the "2014 10-K"). For the quarter, Yahoo announced net income of \$166.34 million, or \$0.17 per diluted share, on revenue of \$1.25 billion, compared to net income of \$348.19 million, or \$0.33 per diluted share, on revenue of \$1.27 billion for the same period in the prior year. For 2014, Yahoo announced net income of \$7.52 billion, or \$7.45 per diluted share, on revenue of \$4.62 billion, compared to net income of \$1.37 billion, or \$1.26 per diluted share, on revenue of \$4.68 billion for 2013.

45. In the 2014 10-K, with respect to the efficacy of the Company's encryption of user data, Yahoo simply stated, in part:

1 *If our security measures are breached, our products and services may be perceived as*
2 *not being secure, users and customers may curtail or stop using our products and*
3 *services, and we may incur significant legal and financial exposure.*

4 Our products and services involve the storage and transmission of Yahoo's users' and
5 customers' personal and proprietary information in our facilities and on our equipment,
6 networks and corporate systems. Security breaches expose us to a risk of loss of this
7 information, litigation, remediation costs, increased costs for security measures, loss of
8 revenue, damage to our reputation, and potential liability. Outside parties may attempt to
9 fraudulently induce employees, users, or customers to disclose sensitive information to
10 gain access to our data or our users' or customers' data. In addition, hardware, software
11 or applications we procure from third parties may contain defects in design or
12 manufacture or other problems that could unexpectedly compromise network and data
13 security. Security breaches or unauthorized access have resulted in and may in the future
14 result in a combination of significant legal and financial exposure, increased remediation
15 and other costs, damage to our reputation and a loss of confidence in the security of our
16 products, services and networks that could have an adverse effect on our business. We
17 take steps to prevent unauthorized access to our corporate systems, however, because the
18 techniques used to obtain unauthorized access, disable or degrade service, or sabotage
19 systems change frequently or may be designed to remain dormant until a triggering event,
20 we may be unable to anticipate these techniques or implement adequate preventative
21 measures. If an actual or perceived breach of our security occurs, the market perception
22 of the effectiveness of our security measures could be harmed and we could lose users
23 and customers.

24 46. The 2014 10-K contained signed certifications pursuant to SOX by the Individual
25 Defendants, stating that the financial information contained in the 2014 10-K was accurate and
26 disclosed any material changes to the Company's internal control over financial reporting.

27 47. On May 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
28 announcing the Company's financial and operating results for the quarter ended March 31, 2015 (the
"Q1 2015 10-Q"). For the quarter, Yahoo announced net income of \$21.20 million, or \$0.02 per
diluted share, on revenue of \$1.23 billion, compared to net income of \$311.58 million, or \$0.29 per
diluted share, on revenue of \$1.13 billion for the same period in the prior year.

48. In the Q1 2015 10-Q, with respect to the efficacy of the Company's encryption of user
data, Yahoo simply stated, in part:

If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.

Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.

49. The Q1 2015 10-Q contained signed certifications pursuant to SOX by the Individual Defendants, stating that the financial information contained in the Q1 2015 10-Q was accurate and disclosed any material changes to the Company's internal control over financial reporting.

50. The statements referenced in ¶¶ 29-49 above were materially false and/or misleading because they misrepresented and/or failed to disclose the following adverse facts pertaining to the Company's business, operational and financial results, which were known to Defendants or recklessly disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (i) Yahoo's information security protocols were inadequate; (ii) Yahoo failed to encrypt its users' personal information and/or failed to encrypt its users' personal data with an up-to-date and secure encryption scheme; (iii) consequently, sensitive personal account information from more than 1 billion users was vulnerable to theft; (iv) a data breach resulting in the theft of personal user data would

foreseeably cause a significant drop in user engagement with Yahoo's websites and services; and (v) as a result, Yahoo's public statements were materially false and misleading at all relevant times.

The Truth Begins to Emerge

51. On July 28, 2015, Ramses Martinez, Yahoo's interim CISO, posted a report on Yahoo's Tumblr blogging platform, entitled "Yahoo's Pays \$1M to Network Vulnerability Reporters," providing some details on Yahoo's "Bug Bounty" program, which Ramses described as "a feedback loop to determine the effectiveness of our application security controls." Ramses' report stated, in part:

Below are some key data points from our Bug Bounty program to date, which we'll continue to update to help the security community understand the efficacy of this work and help focus research in this space:

- To date, we've paid out +\$1M to security vulnerability reporters.
- Submissions since the inception of the program have now reached the 10,000 mark.
- Approximately 1,500 of these 10,000 reports have resulted in a bounty payout.
- The current monthly validity rate of submissions is around 15%, an increase from 10% at the end of 2014.
- More than 1,800 reporters have participated in the program, about 600 of these have reported verifiable bugs.
- 50% of the submissions are from the top 6% set of contributors
- 87% of researchers submit less than 10 bugs, this equates to about 34% of all submissions.

52. Following Martinez's posting, Yahoo's share price fell \$0.17, or 0.45% over the following two trading days, to close at \$36.67 on July 29, 2015.

53. On August 4, 2015, the technology blog *Malwarebytes* reported "a large scale attack abusing Yahoo!'s own ad network." *Malwarebytes* stated, in relevant part:

June and July have set new records for malvertising attacks. We have just uncovered a large scale attack abusing Yahoo!'s own ad network.

As soon as we detected the malicious activity, we notified Yahoo! and we are pleased to report that they took immediate action to stop the issue. The campaign is no longer active at the time of publishing this blog.

1 This latest campaign started on July 28th, as seen from our own telemetry. According to
2 data from SimilarWeb, *Yahoo!’s website has an estimated 6.9 Billion visits per month*
3 *making this one of the largest malvertising attacks we have seen recently.*

4 ...

5 We would like to thank Yahoo! for their prompt response with this incident. Here’s their
6 official statement:

7 “Yahoo is committed to ensuring that both our advertisers and users have a safe
8 and reliable experience. As soon as we learned of this issue, our team took action
9 and will continue to investigate this issue.

10 Unfortunately, disruptive ad behavior affects the entire tech industry. Yahoo has a
11 long history of engagement on this issue and is committed to working with our
12 peers to create a secure advertising experience. We’ll continue to ensure the
13 quality and safety of our ads through our automated testing and through the
14 SafeFrame working group, which seeks to protect consumers and publishers from
15 the potential security risks inherent in the online ad ecosystem.”

16 54. On September 11, 2015, the online publication *TechCrunch* reported that Yahoo’s
17 interim chief information security officer, Ramses Martinez, “quietly left the company in August for a
18 security role at Apple.” *TechCrunch* reported, in relevant part:

19 The news of Martinez departing Yahoo and joining Apple had not been announced but
20 the details are confirmed in his LinkedIn profile, which notes that he joined Apple in
21 August of this year as part of the Cupertino company’s information security team.

22 Reached for comment, Yahoo says that it is currently looking for a permanent CISO.
23 “SVP Jay Rossiter is guiding our security team while we continue our search for Yahoo’s
24 next CISO,” said a spokesperson for the company.

25 Martinez had only been appointed to the role in July, when the former CISO, Alex
26 Stamos, was poached by Facebook. He had been with the company since 2011.

27 At a time when cybersecurity has been a[n] increasing issue due to hacking incidents and
28 developments involving the NSA and snooping by government authorities, Martinez
oversaw a number of security initiatives at Yahoo.

They included the company’s corporate incident response policy, risk analysis process,
threat matrix, and standards; creating and managing the company’s global incident
response program; liaising with law enforcement during security incidents and
investigations; and founding and managing the company’s bug bounty program.

1 55. On this news, Yahoo's share price fell \$1.11, or 3.53%, to close at \$30.32 on September
2 14, 2015, the following trading day.

3 56. On August 7, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
4 announcing the Company's financial and operating results for the quarter ended June 30, 2015 (the "Q2
5 2015 10-Q"). For the quarter, Yahoo announced a net loss of \$21.55 million, or \$0.02 per diluted
6 share, on revenue of \$1.24 billion, compared to net income of \$269.71 million, or \$0.26 per diluted
7 share, on revenue of \$1.08 billion for the same period in the prior year.

8 57. In the Q2 2015 10-Q, with respect to the efficacy of the Company's encryption of user
9 data, Yahoo simply stated, in part:
10

11 ***If our security measures are breached, our products and services may be perceived as***
12 ***not being secure, users and customers may curtail or stop using our products and***
13 ***services, and we may incur significant legal and financial exposure.***

14 Our products and services involve the storage and transmission of Yahoo's users' and
15 customers' personal and proprietary information in our facilities and on our equipment,
16 networks and corporate systems. Security breaches expose us to a risk of loss of this
17 information, litigation, remediation costs, increased costs for security measures, loss of
18 revenue, damage to our reputation, and potential liability. Outside parties may attempt to
19 fraudulently induce employees, users, or customers to disclose sensitive information to
20 gain access to our data or our users' or customers' data. In addition, hardware, software
21 or applications we procure from third parties may contain defects in design or
22 manufacture or other problems that could unexpectedly compromise network and data
23 security. Security breaches or unauthorized access have resulted in and may in the future
24 result in a combination of significant legal and financial exposure, increased remediation
25 and other costs, damage to our reputation and a loss of confidence in the security of our
26 products, services and networks that could have an adverse effect on our business. We
27 take steps to prevent unauthorized access to our corporate systems, however, because the
28 techniques used to obtain unauthorized access, disable or degrade service, or sabotage
systems change frequently or may be designed to remain dormant until a triggering event,
we may be unable to anticipate these techniques or implement adequate preventative
measures. If an actual or perceived breach of our security occurs, the market perception
of the effectiveness of our security measures could be harmed and we could lose users
and customers.

1 58. The Q2 2015 10-Q contained signed certifications pursuant to SOX by the Individual
2 Defendants, stating that the financial information contained in the Q2 2015 10-Q was accurate and
3 disclosed any material changes to the Company's internal control over financial reporting.

4 59. On November 5, 2015, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
5 announcing the Company's financial and operating results for the quarter ended September 30, 2015
6 (the "Q3 2015 10-Q"). For the quarter, Yahoo announced net income of \$76.26 million, or \$0.08 per
7 diluted share, on revenue of \$1.23 billion, compared to net income of \$6.77 billion, or \$6.70 per diluted
8 share, on revenue of \$1.15 billion for the same period in the prior year.

9 60. In the Q3 2015 10-Q, with respect to the efficacy of the Company's encryption of user
10 data, Yahoo simply stated, in part:
11

12 ***If our security measures are breached, our products and services may be perceived as***
13 ***not being secure, users and customers may curtail or stop using our products and***
14 ***services, and we may incur significant legal and financial exposure.***

15 Our products and services involve the storage and transmission of Yahoo's users' and
16 customers' personal and proprietary information in our facilities and on our equipment,
17 networks and corporate systems. Security breaches expose us to a risk of loss of this
18 information, litigation, remediation costs, increased costs for security measures, loss of
19 revenue, damage to our reputation, and potential liability. Outside parties may attempt to
20 fraudulently induce employees, users, or customers to disclose sensitive information to
21 gain access to our data or our users' or customers' data. In addition, hardware, software
22 or applications we procure from third parties may contain defects in design or
23 manufacture or other problems that could unexpectedly compromise network and data
24 security. Security breaches or unauthorized access have resulted in and may in the future
25 result in a combination of significant legal and financial exposure, increased remediation
26 and other costs, damage to our reputation and a loss of confidence in the security of our
27 products, services and networks that could have an adverse effect on our business. We
28 take steps to prevent unauthorized access to our corporate systems, however, because the
techniques used to obtain unauthorized access, disable or degrade service, or sabotage
systems change frequently or may be designed to remain dormant until a triggering event,
we may be unable to anticipate these techniques or implement adequate preventative
measures. If an actual or perceived breach of our security occurs, the market perception
of the effectiveness of our security measures could be harmed and we could lose users
and customers.

61. The Q3 2015 10-Q contained signed certifications pursuant to SOX by the Individual Defendants, stating that the financial information contained in the Q3 2015 10-Q was accurate and disclosed any material changes to the Company's internal control over financial reporting.

62. On February 29, 2016, Yahoo filed an Annual Report on Form 10-K with the SEC, announcing the Company's financial and operating results for the quarter and year ended December 31, 2015 (the "2015 10-K"). For the quarter, Yahoo announced a net loss of \$4.43 billion, or \$4.70 per diluted share, on revenue of \$1.27 billion, compared to net income of \$166.34 million, or \$0.17 per diluted share, on revenue of \$1.25 billion for the same period in the prior year. For 2015, Yahoo announced a net loss of \$4.34 billion, or \$4.64 per diluted share, on revenue of \$4.97 billion, compared to net income of \$7.52 billion, or \$7.45 per diluted share, on revenue of \$4.62 billion for 2014.

63. In the 2015 10-K, with respect to the efficacy of the Company's encryption of user data, Yahoo simply stated, in part:

If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.

Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Additionally, some third parties, such as our distribution partners, service providers and vendors, and app developers, may receive or store information provided by us or by our users through applications integrated with Yahoo. If these third parties fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used or disclosed. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the

1 techniques used to obtain unauthorized access, disable or degrade service, or sabotage
2 systems change frequently or may be designed to remain dormant until a triggering event,
3 we may be unable to anticipate these techniques or implement adequate preventative
4 measures. If an actual or perceived breach of our security occurs, the market perception
of the effectiveness of our security measures could be harmed and we could lose users
and customers.

5 64. The 2015 10-K contained signed certifications pursuant to SOX by the Individual
6 Defendants, stating that the financial information contained in the 2015 10-K was accurate and
7 disclosed any material changes to the Company's internal control over financial reporting.

8 65. On May 10, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
9 announcing the Company's financial and operating results for the quarter ended March 31, 2016 (the
10 "Q1 2016 10-Q"). For the quarter, Yahoo announced a net loss of \$99.23 million, or \$0.10 per diluted
11 share, on revenue of \$1.09 billion, compared to net income of \$21.20 million, or \$0.02 per diluted
12 share, on revenue of \$1.23 billion for the same period in the prior year.

13 66. In the Q1 2016 10-Q, with respect to the efficacy of the Company's encryption of user
14 data, Yahoo simply stated, in part:
15

16 ***If our security measures are breached, our products and services may be perceived as***
17 ***not being secure, users and customers may curtail or stop using our products and***
18 ***services, and we may incur significant legal and financial exposure.***

19 Our products and services involve the storage and transmission of Yahoo's users' and
20 customers' personal and proprietary information in our facilities and on our equipment,
21 networks and corporate systems. Security breaches expose us to a risk of loss of this
22 information, litigation, remediation costs, increased costs for security measures, loss of
23 revenue, damage to our reputation, and potential liability. Outside parties may attempt to
24 fraudulently induce employees, users, or customers to disclose sensitive information to
25 gain access to our data or our users' or customers' data. In addition, hardware, software
26 or applications we procure from third parties may contain defects in design or
27 manufacture or other problems that could unexpectedly compromise network and data
28 security. Additionally, some third parties, such as our distribution partners, service
providers and vendors, and app developers, may receive or store information provided by
us or by our users through applications integrated with Yahoo. If these third parties fail to
adopt or adhere to adequate data security practices, or in the event of a breach of their
networks, our data or our users' data may be improperly accessed, used or disclosed.
Security breaches or unauthorized access have resulted in and may in the future result in
a combination of significant legal and financial exposure, increased remediation and

1 other costs, damage to our reputation and a loss of confidence in the security of our
2 products, services and networks that could have an adverse effect on our business. We
3 take steps to prevent unauthorized access to our corporate systems, however, because the
4 techniques used to obtain unauthorized access, disable or degrade service, or sabotage
5 systems change frequently or may be designed to remain dormant until a triggering event,
6 we may be unable to anticipate these techniques or implement adequate preventative
7 measures. If an actual or perceived breach of our security occurs, the market perception
8 of the effectiveness of our security measures could be harmed and we could lose users
9 and customers.

10 67. The Q1 2016 10-Q contained signed certifications pursuant to SOX by the Individual
11 Defendants, stating that the financial information contained in the Q1 2016 10-Q was accurate and
12 disclosed any material changes to the Company's internal control over financial reporting.

13 68. On July 25, 2016, Verizon formally announced its intent to acquire Yahoo's internet
14 business for \$4.8 billion.

15 69. On August 8, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
16 announcing the Company's financial and operating results for the quarter ended June 30, 2016 (the "Q2
17 2016 10-Q"). For the quarter, Yahoo announced a net loss of \$439.91 million, or \$0.46 per diluted
18 share, on revenue of \$1.31 billion, compared to a net loss of \$21.55 million, or \$0.02 per diluted share,
19 on revenue of \$1.24 billion for the same period in the prior year.

20 70. In the Q2 2016 10-Q, with respect to the efficacy of the Company's encryption of user
21 data, Yahoo simply stated, in part:

22 ***If our security measures are breached, our products and services may be perceived as
23 not being secure, users and customers may curtail or stop using our products and
24 services, and we may incur significant legal and financial exposure.***

25 Our products and services involve the storage and transmission of Yahoo's users' and
26 customers' personal and proprietary information in our facilities and on our equipment,
27 networks and corporate systems. Security breaches expose us to a risk of loss of this
28 information, litigation, remediation costs, increased costs for security measures, loss of
revenue, damage to our reputation, and potential liability. Outside parties may attempt to
fraudulently induce employees, users, or customers to disclose sensitive information to
gain access to our data or our users' or customers' data. In addition, hardware, software
or applications we procure from third parties may contain defects in design or
manufacture or other problems that could unexpectedly compromise network and data

1 security. Additionally, some third parties, such as our distribution partners, service
2 providers and vendors, and app developers, may receive or store information provided by
3 us or by our users through applications integrated with Yahoo. If these third parties fail to
4 adopt or adhere to adequate data security practices, or in the event of a breach of their
5 networks, our data or our users' data may be improperly accessed, used or disclosed.
6 Security breaches or unauthorized access have resulted in and may in the future result in
7 a combination of significant legal and financial exposure, increased remediation and
8 other costs, damage to our reputation and a loss of confidence in the security of our
9 products, services and networks that could have an adverse effect on our business. We
10 take steps to prevent unauthorized access to our corporate systems, however, because the
11 techniques used to obtain unauthorized access, disable or degrade service, or sabotage
12 systems change frequently or may be designed to remain dormant until a triggering event,
13 we may be unable to anticipate these techniques or implement adequate preventative
14 measures. If an actual or perceived breach of our security occurs, the market perception
15 of the effectiveness of our security measures could be harmed and we could lose users
16 and customers.

17 71. The Q2 2016 10-Q contained signed certifications pursuant to SOX by the Individual
18 Defendants, stating that the financial information contained in the Q2 2016 10-Q was accurate and
19 disclosed any material changes to the Company's internal control over financial reporting.

20 72. On September 22, 2016, Yahoo disclosed that hackers had stolen information in late
21 2014 on more than 500 million accounts. Following the breach, Yahoo executives advised investors
22 that the breach was not material, in part because the Company had not required to reset their passwords.

23 73. On this news, Yahoo's share price fell \$1.35, or 3.06%, to close at \$42.80 on September
24 23, 2016.

25 74. On November 9, 2016, Yahoo filed a Quarterly Report on Form 10-Q with the SEC,
26 announcing in full the Company's financial and operating results for the quarter ended September 30,
27 2016 (the "Q3 2016 10-Q"). For the quarter, Yahoo announced net income of \$162.83 million, or
28 \$0.17 per diluted share, on revenue of \$1.31 billion, compared to net income of \$76.26 million, or
\$0.08 per diluted share, on revenue of \$1.23 billion for the same period in the prior year.

75. In the Q3 2016 10-Q, with respect to the efficacy of the Company's encryption of user
data, Yahoo stated, in part:

1 On September 22, 2016, we disclosed that, based on an ongoing investigation, a copy of
2 certain user account information for at least 500 million user accounts was stolen from
3 Yahoo's network in late 2014 (the "Security Incident"). We believe the user account
4 information was stolen by a state-sponsored actor. The user account information taken
5 included names, email addresses, telephone numbers, dates of birth, hashed passwords
6 (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security
7 questions and answers. Our investigation to date indicates that the stolen information did
8 not include unprotected passwords, payment card data, or bank account information.
9 Payment card data and bank account information are not stored in the system that the
10 investigation found to be affected. Based on the investigation to date, we do not have
11 evidence that the state-sponsored actor is currently in or accessing the Company's
12 network.

13 ...

14 ***Our security measures may be breached as they were in the Security Incident and user***
15 ***data accessed, which may cause users and customers to curtail or stop using our***
16 ***products and services, and may cause us to incur significant legal and financial***
17 ***exposure.***

18 Our products and services involve the storage and transmission of Yahoo's users' and
19 customers' personal and proprietary information in our facilities and on our equipment,
20 networks, and corporate systems. Yahoo is routinely targeted by outside third parties,
21 including technically sophisticated and well-resourced state-sponsored actors, attempting
22 to access or steal our user and customer data or otherwise compromise user accounts. We
23 believe such a state-sponsored actor was responsible for the theft involved in the Security
24 Incident. Security breaches or other unauthorized access or actions expose us to a risk of
25 theft of user data, regulatory actions, litigation, investigations, remediation costs, damage
26 to our reputation and brand, loss of user and partner confidence in the security of our
27 products and services and resulting fees, costs, and expenses, loss of revenue, damage to
28 our reputation, and potential liability. Outside parties may attempt to fraudulently induce
employees, users, partners, or customers to disclose sensitive information or take other
actions to gain access to our data or our users' or customers' data. In addition, hardware,
software, or applications we procure from third parties may contain defects in design or
manufacture or other problems that could unexpectedly compromise network and data
security. In addition, our or our partners' implementation of software may contain
security vulnerabilities or may not be implemented properly due to human error or
limitations in our systems. Additionally, some third parties, such as our distribution
partners, service providers, vendors, and app developers, may receive or store
information provided by us or by our users through applications that are integrated with
Yahoo properties and services. If these third parties fail to adopt or adhere to adequate
data security practices, or in the event of a breach of their networks, our data or our users'
data may be improperly accessed, used, or disclosed. Security breaches or other
unauthorized access (such as the Security Incident) have resulted in, and may in the
future result in, a combination of significant legal and financial exposure, increased
remediation and other costs, damage to our reputation, and a loss of confidence in the
security of our products, services, and networks that could have a significantly adverse

1 effect on our business. We take steps to prevent unauthorized access to our corporate
2 systems, however, because the techniques used to obtain unauthorized access, disable or
3 degrade service, or sabotage systems change frequently or may be disguised or difficult
4 to detect, or designed to remain dormant until a triggering event, we may be unable to
5 anticipate these techniques or implement adequate preventative measures. Breaches of
6 our security measures, such as the Security Incident, or perceived breaches, have caused
7 and may in the future cause, the market perception of the effectiveness of our security
8 measures to be harmed and cause us to lose users and customers.

9 76. The Q3 2016 10-Q contained signed certifications pursuant to SOX by the Individual
10 Defendants, stating that the financial information contained in the Q3 2016 10-Q was accurate and
11 disclosed any material changes to the Company's internal control over financial reporting.

12 77. On December 14, 2016, post-market, post-market, Yahoo announced that it had
13 uncovered a data breach, stating that data from more than 1 billion user accounts was compromised in
14 August 2013. In a press release and Current Report filed with the SEC on Form 8-K, Yahoo stated, in
15 part:

16 SUNNYVALE, Calif., December 14, 2016— Yahoo! Inc. (NASDAQ:YHOO) has
17 identified data security issues concerning certain Yahoo user accounts. Yahoo has taken
18 steps to secure user accounts and is working closely with law enforcement.

19 As Yahoo previously disclosed in November, law enforcement provided the company
20 with data files that a third party claimed was Yahoo user data. The company analyzed this
21 data with the assistance of outside forensic experts and found that it appears to be Yahoo
22 user data. Based on further analysis of this data by the forensic experts, ***Yahoo believes***
23 ***an unauthorized third party, in August 2013, stole data associated with more than one***
24 ***billion user accounts.*** The company has not been able to identify the intrusion associated
25 with this theft. Yahoo believes this incident is likely distinct from the incident the
26 company disclosed on September 22, 2016.

27 ***For potentially affected accounts, the stolen user account information may have***
28 ***included names, email addresses, telephone numbers, dates of birth, hashed passwords***
(using MD5) and, in some cases, encrypted or unencrypted security questions and
answers. The investigation indicates that the stolen information did not include
passwords in clear text, payment card data, or bank account information. Payment card
data and bank account information are not stored in the system the company believes was
affected.

Yahoo is notifying potentially affected users and has taken steps to secure their
accounts, including requiring users to change their passwords. Yahoo has also

1 *invalidated unencrypted security questions and answers so that they cannot be used to*
2 *access an account.*

3 Separately, Yahoo previously disclosed that its outside forensic experts were
4 investigating the creation of forged cookies that could allow an intruder to access users'
5 accounts without a password. Based on the ongoing investigation, the company believes
6 an unauthorized third party accessed the company's proprietary code to learn how to
7 forge cookies. The outside forensic experts have identified user accounts for which they
8 believe forged cookies were taken or used. Yahoo is notifying the affected account
9 holders, and has invalidated the forged cookies. The company has connected some of this
10 activity to the same state-sponsored actor believed to be responsible for the data theft the
11 company disclosed on September 22, 2016.

12 (Emphases added.)

13 78. On this news, Yahoo's share price fell \$2.50, or 6.11%, to close at \$38.41 on December
14 15, 2016.

15 79. On December 15, 2016, after the market closed, the *Wall Street Journal* published an
16 article entitled "Yahoo's Password Move May Put Verizon Deal at Risk." The article stated, in part:

17 Yahoo Inc.'s move to force some users to reset their passwords following a newly
18 disclosed security breach could disrupt the planned sale of its core assets to Verizon
19 Communications Inc., security experts say.

20 Yahoo didn't force users to reset their passwords after its September disclosure of
21 another breach. *Experts say forcing users to reset their passwords typically causes some*
22 *to drop a service.*

23 That is one reason why the newly disclosed hack—which Yahoo says occurred in 2013
24 and affected more than one billion accounts—could prove more disruptive to Verizon's
25 pending \$4.83 billion acquisition of Yahoo's core assets.

26 ...

27 *Yahoo is forcing users to reset their passwords now because some of the material taken*
28 *in the 2013 breach wasn't encrypted, and other parts were protected by what is now*
29 *considered an outdated encryption scheme*, according to a person familiar with that
30 matter.

31 (Emphases added.)

32 80. On January 23, 2017, the *Wall Street Journal* reported that the SEC had opened an
33 investigation into the timing of Yahoo's disclosures regarding the data breaches. The article reported,
34 in part:

1 The Securities and Exchange Commission has opened an investigation, and in December
2 issued requests for documents, as it looks into whether the tech company's disclosures
3 about the cyberattacks complied with civil securities laws, the people said. The SEC
4 requires companies to disclose cybersecurity risks as soon as they are determined to have
5 an effect on investors.

6 The investigation is likely to center on a 2014 data breach at Yahoo that compromised the
7 data of at least 500 million users, according to the people familiar with the matter. Yahoo
8 disclosed that breach in September 2016, despite having linked the incident to state-
9 sponsored hackers two years earlier.

10 To date, Yahoo hasn't explained why the company took two years to disclose the 2014
11 incident publicly or who made the decision not to go public sooner with this information.
12 In mid-December Yahoo also said it had recently discovered an August 2013 data breach
13 that had exposed the private information of more than 1 billion Yahoo users.

14 81. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in
15 the market value of the Company's common shares, Plaintiff and other Class members have suffered
16 significant losses and damages.

17 **PLAINTIFF'S CLASS ACTION ALLEGATIONS**

18 82. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure
19 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired
20 Yahoo common shares traded on the NASDAQ during the Class Period (the "Class"); and were
21 damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are
22 Defendants herein, the officers and directors of the Company, at all relevant times, members of their
23 immediate families and their legal representatives, heirs, successors or assigns and any entity in which
24 Defendants have or had a controlling interest.

25 83. The members of the Class are so numerous that joinder of all members is impracticable.
26 Throughout the Class Period, Yahoo common shares were actively traded on the NASDAQ. While the
27 exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through
28 appropriate discovery, Plaintiff believes that there are hundreds or thousands of members in the
proposed Class. Record owners and other members of the Class may be identified from records

1 maintained by Yahoo or its transfer agent and may be notified of the pendency of this action by mail,
2 using the form of notice similar to that customarily used in securities class actions.

3 84. Plaintiff's claims are typical of the claims of the members of the Class as all members of
4 the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is
5 complained of herein.

6 85. Plaintiff will fairly and adequately protect the interests of the members of the Class and
7 has retained counsel competent and experienced in class and securities litigation. Plaintiff has no
8 interests antagonistic to or in conflict with those of the Class.

9 86. Common questions of law and fact exist as to all members of the Class and predominate
10 over any questions solely affecting individual members of the Class. Among the questions of law and
11 fact common to the Class are:
12

- 13 • whether the federal securities laws were violated by Defendants' acts as alleged
14 herein;
- 15 • whether statements made by Defendants to the investing public during the Class
16 Period misrepresented material facts about the financial condition, business,
17 operations, and management of Yahoo;
- 18 • whether Defendants caused Yahoo to issue false and misleading financial
19 statements during the Class Period;
- 20 • whether Defendants acted knowingly or recklessly in issuing false and
21 misleading financial statements;
- 22 • whether the prices of Yahoo securities during the Class Period were artificially
23 inflated because of Defendants' conduct complained of herein; and
- 24 • whether the members of the Class have sustained damages and, if so, what is the
25 proper measure of damages.

26 87. A class action is superior to all other available methods for the fair and efficient
27 adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the
28 damages suffered by individual Class members may be relatively small, the expense and burden of

1 individual litigation make it impossible for members of the Class to individually redress the wrongs
2 done to them. There will be no difficulty in the management of this action as a class action.

3 88. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-
4 the-market doctrine in that:

- 5 • Defendants made public misrepresentations or failed to disclose material facts
6 during the Class Period;
- 7 • the omissions and misrepresentations were material;
- 8 • Yahoo common shares are traded in efficient markets;
- 9 • the Company's shares were liquid and traded with moderate to heavy volume
10 during the Class Period;
- 11 • the Company traded on the NASDAQ, and was covered by multiple analysts;
- 12 • the misrepresentations and omissions alleged would tend to induce a reasonable
13 investor to misjudge the value of the Company's common shares; and
- 14 • Plaintiff and members of the Class purchased and/or sold Yahoo common shares
15 between the time the Defendants failed to disclose or misrepresented material
16 facts and the time the true facts were disclosed, without knowledge of the
17 omitted or misrepresented facts.

18 89. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a
19 presumption of reliance upon the integrity of the market.

20 90. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of
21 reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United*
22 *States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class
23 Period statements in violation of a duty to disclose such information, as detailed above.
24
25
26
27
28

COUNT I

**Violation of Section 10(b) of The Exchange Act and Rule 10b-5
Against All Defendants**

91. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

92. This Count is asserted against Yahoo and the Individual Defendants and is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

93. During the Class Period, Yahoo and the Individual Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

94. Yahoo and the Individual Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

- employed devices, schemes and artifices to defraud;
- made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or
- engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Yahoo common shares during the Class Period.

95. Yahoo and the Individual Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of Yahoo were materially false and misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws. These

1 Defendants by virtue of their receipt of information reflecting the true facts of Yahoo, their control
2 over, and/or receipt and/or modification of Yahoo allegedly materially misleading statements, and/or
3 their associations with the Company which made them privy to confidential proprietary information
4 concerning Yahoo, participated in the fraudulent scheme alleged herein.

5 96. Individual Defendants, who are the senior officers and/or directors of the Company, had
6 actual knowledge of the material omissions and/or the falsity of the material statements set forth above,
7 and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with
8 reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements
9 made by them or other Yahoo personnel to members of the investing public, including Plaintiff and the
10 Class.
11

12 97. As a result of the foregoing, the market price of Yahoo common shares was artificially
13 inflated during the Class Period. In ignorance of the falsity of Yahoo's and the Individual Defendants'
14 statements, Plaintiff and the other members of the Class relied on the statements described above and/or
15 the integrity of the market price of Yahoo common shares during the Class Period in purchasing Yahoo
16 common shares at prices that were artificially inflated as a result of Yahoo's and the Individual
17 Defendants' false and misleading statements.
18

19 98. Had Plaintiff and the other members of the Class been aware that the market price of
20 Yahoo common shares had been artificially and falsely inflated by Yahoo's and the Individual
21 Defendants' misleading statements and by the material adverse information which Yahoo's and the
22 Individual Defendants did not disclose, they would not have purchased Yahoo's common shares at the
23 artificially inflated prices that they did, or at all.
24

25 99. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the
26 Class have suffered damages in an amount to be established at trial.
27
28

100. By reason of the foregoing, Yahoo and the Individual Defendants have violated Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the other members of the Class for substantial damages which they suffered in connection with their purchase of Yahoo common shares during the Class Period.

COUNT II

Violation of Section 20(a) of The Exchange Act Against The Individual Defendants

101. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

102. During the Class Period, the Individual Defendants participated in the operation and management of Yahoo, and conducted and participated, directly and indirectly, in the conduct of Yahoo's business affairs. Because of their senior positions, they knew the adverse non-public information regarding the Company's inadequate internal safeguards in data security protocols.

103. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Yahoo's financial condition and results of operations, and to correct promptly any public statements issued by Yahoo which had become materially false or misleading.

104. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which Yahoo disseminated in the marketplace during the Class Period. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Yahoo to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of Yahoo within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Yahoo common shares.

105. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by Yahoo.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against Defendants as follows:

A. Determining that the instant action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and certifying Plaintiff as the Class representative;

B. Requiring Defendants to pay damages sustained by Plaintiff and the Class by reason of the acts and transactions alleged herein;

C. Awarding Plaintiff and the other members of the Class prejudgment and post-judgment interest, as well as their reasonable attorneys' fees, expert fees and other costs; and

D. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

Dated: March 21, 2017

Respectfully submitted,

POMERANTZ LLP

By: /s/ Jennifer Pafiti
Jennifer Pafiti (SBN 282790)
468 North Camden Drive
Beverly Hills, CA 90210
Telephone: (818) 532-6499
Email: jpafiti@pomlaw.com

POMERANTZ, LLP

Jeremy A. Lieberman
J. Alexander Hood II
Hui M. Chang
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
Email: jalieberman@pomlaw.com

Email: ahood@pomlaw.com
Email: hchang@pomlaw.com

POMERANTZ LLP

Patrick V. Dahlstrom
Ten South La Salle Street, Suite 3505
Chicago, Illinois 60603
Telephone: (312) 377-1181
Facsimile: (312) 377-1184
Email: pdahlstrom@pomlaw.com

**BRONSTEIN, GEWIRTZ
& GROSSMAN, LLC**

Peretz Bronstein
60 East 42nd Street, Suite 4600
New York, NY 10165
Telephone: (212) 697-6484
Facsimile (212) 697-7296
Email: peretz@bgandg.com

Attorneys for Plaintiff

Submission Date

2017-01-26 11:10:13

CERTIFICATION PURSUANT TO FEDERAL SECURITIES LAWS

1. I make this declaration pursuant to Section 27(a)(2) of the Securities Act of 1933 ("Securities Act") and/or Section 21D(a)(2) of the Securities Exchange Act of 1934 ("Exchange Act") as amended by the Private Securities Litigation Reform Act of 1995.
2. I have reviewed a Complaint against Yahoo! Inc. ("Yahoo" or the "Company"), and authorize the filing of a comparable complaint on my behalf.
3. I did not purchase or acquire Yahoo securities at the direction of plaintiffs' counsel or in order to participate in any private action arising under the Securities Act or Exchange Act.
4. I am willing to serve as a representative party on behalf of a Class of investors who purchased or acquired Yahoo securities during the class period, including providing testimony at deposition and trial, if necessary. I understand that the Court has the authority to select the most adequate lead plaintiff in this action.
5. To the best of my current knowledge, the attached sheet lists all of my transactions in Yahoo securities during the Class Period as specified in the Complaint.
6. During the three-year period preceding the date on which this Certification is signed, I have not sought to serve as a representative party on behalf of a class under the federal securities laws.
7. I agree not to accept any payment for serving as a representative party on behalf of the class as set forth in the Complaint, beyond my pro rata share of any recovery, except such reasonable costs and expenses directly relating to the representation of the class as ordered or approved by the Court.
8. I declare under penalty of perjury that the foregoing is true and correct.

Name

Print Name

Nafiz Talukder

Acquisitions

Configurable list (if none enter none)

Date Acquired	Number of Shares Acquired	Price per Share Acquired
09/15/2014	457	43.73
09/15/2014	273	43.54
11/04/2014	633	46.15
11/05/2014	373	47.84
11/06/2014	493	46.84
06/13/2016	410	36.50
08/26/2016	70	41.97

Sales


Configurable list (if none enter none)

Date Sold	Number of Shares Sold	Price per Share Sold
11/04/2014	730	45.70
11/04/2014	633	45.70
07/17/2015	333	39.72

Documents & Message

Upload your brokerage statements showing your individual purchase and sale orders.

(redacted)




Signature



Full Name

Nafiz Talukder

(redacted)



YAHOO! INC (YHOO)

Talukder, Nafiz

LIST OF PURCHASES AND SALES

DATE	PURCHASE OR SALE	NUMBER OF SHS/UTS	PRICE PER SH/UT
9/15/2014	Purchase	457	\$43.7300
9/15/2014	Purchase	273	\$43.5400
11/4/2014	Purchase	633	\$46.1500
11/5/2014	Purchase	373	\$47.8355
11/6/2014	Purchase	493	\$46.8377
6/13/2016	Purchase	410	\$36.4999
8/26/2016	Purchase	70	\$41.9676
11/4/2014	Sale	730	\$45.7000
11/4/2014	Sale	633	\$45.7000
7/17/2015	Sale	333	\$39.7200